



Online Banking Services Fraud Information Alert

MIAA Anti-Fraud Service

August 2023

Advice to NHS staff and NHS Suppliers

What is online banking?

Banking online means accessing your bank account and carrying out financial transactions through the internet on your smartphone, tablet or computer. It's quick, usually free and allows you to do tasks, such as paying bills and transferring money, without having to visit a physical branch or call your bank.

Many traditional banks also have free apps which let you use their services from your smartphone or tablet.

In the UK the bank regulators are the Financial Conduct Authority and the Prudential Regulation Authority and they set the financial compensation limits and compensation rules for banks regulated in UK. Banks registered in the UK that offer on-line banking have the advantage that your bank account is protected by the Financial Services Compensation Scheme (FSCS). To see a full list of banks and building societies that offer banking services that are considered banks by the Prudential Regulation Authority go to [List of UK Banks](#).

Online Banks - The associated fraud risks NHS bodies, NHS staff and NHS Suppliers face if banking online and some questions to ask yourself

- There will be no physical bank branch or head office (and maybe no presence in the UK at all) where complaints can be made should something go wrong.
- Does the online bank website give any headquarters or registered address?
- The online bank may offer no contact telephone number and only communicate by email / instant message / online messaging.
- If your email or account has been compromised, in what way can you then securely contact / liaise with your bank if you think there is a problem with your account?
- How would they be able contact you if there was a problem with your bank account if either your account or email has been compromised?
- How secure is online messaging if your account has been compromised?
- The online bank may not have an established fraud team to assist with such queries from customers and they may be difficult to contact. Contact may only be via a call centre with inexperienced operatives, and may lead to delays in a time where a quick response is imperative.
- Check if an online bank has had any adverse publicity by carrying out some due diligence, such as with consumer champion websites or similar. And if so, what concerns were raised and how were these resolved - if they have been?

Continued on page 2

ACTION REQUIRED

MIAA Anti-Fraud Service recommend this alert is distributed to:

**NHS Staff and
Suppliers
for
ACTION &
AWARENESS**

MIAA Anti-Fraud 23/24 1

For further information on MIAA's Anti-Fraud Service visit miao.nhs.uk

Please note this alert is not an endorsement to promote any bank. The sole aim is to advise NHS Staff and NHS Suppliers of the potential risks/ limitations of using an online bank.

How secure is online banking? Keeping your online account safe

UK regulated banks should take precautions to make sure your online account is safe. These include encrypted websites, timed log outs and many authentication processes. You can ask your bank for more details.

Accessing your bank account online is generally safe. This is as long as you make sure you enter in all the right details when making a transaction and follow a few rules:

- Ensure you download such an app from an official app store such as Google or from Apple App stores.
- Check your statement often and report any unusual activity to your bank.
- Don't reply to emails that claim to be from your bank that ask for personal details or passwords.
- Always remember to log out of your online banking session.
- Only use secure wi-fi connections to access your bank account.
- Public wi-fi connections are often not secure, so it's important not to use them for banking or to make purchases. If you're out and about with a mobile or tablet, it's safer to use your 3G or 4G connection.
- Keep your operating system and anti-virus software up to date.
- Choose your password carefully – create it by combining three random words, and using a combination of letters, numbers and special characters, and don't re-use the same one for different accounts.

Read more about safe online banking on the [Get Safe Online website](#). Find information about [Shopping and paying safely online](#).

What to do if you're a victim of online bank fraud

Check your account online regularly to spot any irregularities and contact your online bank as soon as possible if you think you've been a victim of fraud.

Contact [Action Fraud](#) on 0300 123 2040 - They may be limited in what help they can offer if your online bank is overseas.

All UK based banks are legally required to refund unauthorised transactions and restore your account to the state it would have been in had the transaction not be made unless it can prove that you've acted fraudulently or been grossly negligent.

A UK bank can't refuse to refund you based on a hunch – they must investigate properly.

If you're unhappy with the way your UK regulated bank has dealt with your complaint, you can refer the matter to the Financial Ombudsman Service (FOS). For overseas online banks you will need to check if such a scheme exists.

If using an overseas-based online bank, check it is appropriately regulated and offers a compensation scheme. If you suspect financial crime/ fraud report it to the police of the country your overseas bank is based in.

Please note this alert is not an endorsement to promote any bank. The sole aim is to advise NHS Staff and NHS Suppliers of the potential risks/ limitations of using an online bank.